Department : **Computer Science and Engineering.**

Year & Semester : **IV/VII**

Sub Code & Sub Name : **20CSE472B & Cyber Security**

Unit-I

S.No	Part-A Questions(2 marks)
1.	Define cybercrime.
2.	Who is a cybercriminal?
3.	Give two examples of financial cybercrimes.
4.	State one major reason for the need of cyberlaws in India.
5.	Expand ITA. When was it enacted?
6.	Mention one positive aspect of ITA 2000.
7.	Mention one weak area of ITA 2000.
8.	Which amendment of ITA made e-records legally admissible?
9.	Name any two common classifications of cybercrimes.
10.	Write one example of intellectual property in cyberspace.
11.	What is phishing?
12.	Name any one section of ITA 2000 related to hacking.
13.	Give one global initiative against cybercrime.
14.	State one ethical issue related to cybercrime.
15.	Define digital signature as per ITA 2000.

S.No	Part-B Questions(10 Marks)
1.	Explain the relationship between cybercrime and information security. How do they complement each other in the digital ecosystem?
2.	Discuss the different categories of cybercriminals with suitable examples.
3.	Classify cybercrimes into major types and explain each with relevant case studies.
4.	Why are cyberlaws essential in the Indian context? Highlight with examples.
5.	Discuss the legal perspectives of cybercrime at national and international levels.
6.	Evaluate the Indian perspective of cybercrimes with reference to recent incidents.
7.	Explain the provisions of the Indian IT Act 2000 related to cybercrimes.
8.	Analyze the positive aspects and weak areas of the ITA 2000.
9.	Describe the key amendments made to the Indian IT Act 2000 for admissibility of electronic records.
10.	Discuss the important amendments made to the Indian IT Act 2008 and their impact.
11.	Explain the global perspective on cybercrimes. How do international laws address them?
12.	What is Intellectual Property in cyberspace? Explain issues of copyright, trademark, and patent in the digital world.
13.	Discuss the ethical dimensions of cybercrimes with examples of ethical dilemmas faced by professionals.

14.	Compare and contrast the Indian IT Act with international cybercrime laws.
15.	Suggest strategies for strengthening India’s legal framework against cybercrimes.

Unit-II

S.No	Part-A Questions(2 Marks)
1.	Define cybercrime categories with one example.
2.	What is an attack vector?
3.	State one method used by cybercriminals to plan an attack.
4.	Define social engineering.
5.	What is cyberstalking?
6.	How can cybercafes become hotspots for cybercrime?
7.	Define botnet.
8.	Mention one cloud computing security concern.
9.	Define phishing.
10.	What is spear phishing?
11.	Give one example of a phishing scam.
12.	What is a phishing toolkit?
13.	Define spy phishing.
14.	What is identity theft?
15.	What is Personally Identifiable Information (PII)? Give one example.

S.No	Part-B Questions(10 Marks)
1.	Explain different categories of cybercrime with suitable examples.
2.	Describe how cybercriminals plan and execute their attacks.
3.	Discuss the techniques of social engineering and its impact on individuals and organizations.
4.	What is cyberstalking? Explain its types, methods, and preventive measures.
5.	Discuss the role of cybercafes in cybercrimes. Suggest countermeasures to regulate their misuse.
6.	Explain botnets. How are they created and used in cyberattacks?
7.	Define attack vectors. Discuss major types of attack vectors with examples.
8.	Examine the security issues in cloud computing and measures to overcome them.
9.	Explain phishing methods and techniques with real-world case studies.
10.	What is spear phishing? How is it different from regular phishing? Discuss preventive measures.
11.	Discuss various phishing scams and their impact on society.
12.	Explain phishing toolkits and their role in automating phishing attacks.
13.	What is spy phishing? Explain its working mechanism and preventive strategies.
14.	Explain identity theft: types, techniques used by criminals, and countermeasures.
15.	Discuss the concept of effacing online identity. Why do criminals do it and how can it be prevented?

Unit-III

S.No	Part-A Questions(2 Marks)
1.	What is meant by proliferation of mobile and wireless devices?
2.	Mention one trend in mobility.
3.	Define mobile computing.
4.	State one example of credit card fraud in mobile transactions.
5.	List one security challenge posed by mobile devices.
6.	What is the role of registry settings in mobile device security?
7.	Define authentication service security.
8.	Mention one common attack on mobile/cell phones.
9.	What is SIM cloning?
10.	State one organizational risk due to mobile devices.
11.	What is mobile malware?
12.	Define BYOD (Bring Your Own Device).
13.	Mention one organizational measure for handling mobile device security.
14.	What is mobile phishing?
15.	State one example of wireless connectivity used in mobile devices.

S.No	Part-B Questions(10 Marks)
1.	Explain the proliferation of mobile and wireless devices in recent years.
2.	Discuss the latest trends in mobility and their impact on society.
3.	Describe credit card frauds in the mobile and wireless computing era with examples.
4.	Discuss in detail the major security challenges posed by mobile devices.
5.	What are registry settings for mobile devices? Explain how they affect security.
6.	Explain authentication service security in the context of mobile devices.
7.	Discuss various types of attacks on mobile/cell phones with examples.
8.	Analyze the security implications of mobile devices for organizations.
9.	Suggest organizational measures for handling mobile device–related security issues.
10.	Discuss the risks and countermeasures of mobile malware.
11.	Explain SIM cloning attacks and their prevention techniques.
12.	Discuss the security issues arising from BYOD policies in organizations.
13.	Explain mobile phishing techniques and their countermeasures.
14.	Evaluate the organizational challenges of securing wireless connectivity in mobile environments.
15.	Suggest a comprehensive security framework for mobile device management in enterprises.

Unit-IV

S.No	Part-A Questions(2 Marks)
1.	What is a proxy server?
2.	Define anonymizer.
3.	State one use of proxy servers in cybersecurity.
4.	What is password cracking?
5.	Name one common password cracking tool.
6.	Define keylogger.
7.	What is spyware?
8.	Differentiate between virus and worm.
9.	What is a Trojan horse in computing?
10.	Define backdoor.
11.	What is steganography?
12.	Expand DoS and DDoS.
13.	Define SQL Injection in one sentence.
14.	What is buffer overflow?
15.	Mention one type of attack on wireless networks.

S.No	Part-B Questions(10 Marks)
1.	Explain proxy servers and anonymizers. Discuss their role in cybersecurity and privacy.
2.	Describe different password cracking techniques with examples.
3.	Discuss the working of keyloggers. How do they compromise user security?
4.	Explain spyware: types, techniques of spreading, and prevention methods.
5.	Differentiate between viruses and worms with examples
6.	What are Trojan horses and backdoors? Explain with real-world incidents.
7.	Explain steganography. How is it used for hiding malicious content?
8.	Discuss Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks with suitable examples.
9.	Explain SQL Injection attacks. How do they compromise databases? Discuss countermeasures.
10.	What is buffer overflow? Explain its mechanism with examples
11.	Discuss various attacks on wireless networks and their preventive measures.
12.	Explain how proxy servers can be misused by cybercriminals and suggest safeguards.
13.	Write detailed notes on modern spyware threats and their impact on organizations.
14.	Analyze the role of Trojans in advanced persistent threats (APT).
15.	Discuss a case study of a major DDoS or SQL Injection attack and its consequences.

Unit-V

S.No	Part-A Questions(2 Marks)
1.	Define cyberforensics.
2.	What is digital evidence?
3.	Mention one objective of cyberforensics.
4.	State one tool used for smartphone forensics.
5.	What is EnCase used for in digital forensics?
6.	Define device seizure in cyberforensics.
7.	What is MOBILedit?
8.	Give one example of cyberforensics analysis of emails.
9.	Mention one type of cybercrime that can be investigated via social networking sites.
10.	State one real-life example of online scams in India.
11.	What is an online cheque cashing scam?
12.	Define intellectual property crime in the cyber context.
13.	Give one example of a mini-case of online gambling in India.
14.	Mention one Indian bank cybercrime incident.
15.	What is the importance of smartphone forensics in investigations?

S.No	Part-B Questions(10 Marks)
1.	Explain cyberforensics and its significance in modern investigations.
2.	Discuss cyberforensics and digital evidence. How is evidence collected and preserved?
3.	Explain the process of forensic analysis of emails with an example.
4.	Discuss forensics and social networking sites: methods to investigate crimes.
5.	Explain smartphone forensics and its importance in cybercrime investigation.
6.	Describe the role of EnCase in digital forensics.
7.	Explain device seizure procedures in cyberforensics investigations.
8.	Discuss the use of MOBILedit in extracting data from handheld devices.
9.	Analyze a real-life cybercrime example: Official website of Maharashtra Government hacked.
10.	Discuss the Indian banks cybercrime incident: losses and preventive measures.
11.	Explain the case of game source code theft and its implications.
12.	Describe an Indian case of online gambling and the forensic approach used.
13.	Explain an Indian case of intellectual property crime and investigative measures.
14.	Discuss online scams like cheque cashing and charity scams with preventive strategies.
15.	Suggest a framework for handling cybercrime investigations involving handheld devices and online scams.